

IN THE CLAIMS:

Please amend the claims as follows:

1. (Currently Amended) A method of automatically identifying anomalous situations during system operations, said method comprising:
 - recording features of normal system operations ~~actions performed by a system as~~ features in a history file;
 - automatically creating a model for each of said features of said normal system operations ~~only from normal data~~ in said history file;
 - ~~determining by~~ calculating anomaly scores of said features of said normal system ~~operations and storing said anomaly scores in to produce~~ a trained file;
 - establishing a threshold to evaluate whether events in live system operations are ~~anomalies as compared to said normal system operations features are abnormal~~;
 - automatically identifying ~~abnormal actions~~ anomalous events in ~~of said live system~~ operations based on said anomaly scores and on said threshold;
 - reporting said anomalous events; and
 - periodically repeating said calculating determining, ~~wherein said abnormal actions indicate anomalous situations during system operation.~~
2. (Currently Amended) The method in claim 1, wherein said creating ~~said model for said~~ each feature comprises:
 - establishing relationships that exist between each of said ~~each~~ features ~~for~~ of said normal

10/658,623

2

system operations;

selecting a labeled feature from said features;

mathematically rearranging said relationships from the point of view of said labeled feature to create a solution for said labeled feature, wherein said solution comprises a model for said labeled feature;

selecting different features as said labeled feature and repeating said process of mathematically rearranging said relationships to produce solutions from the point of view of each remaining feature as models for the remaining features.

3. (Original) The method in claim 2, wherein said solution comprises a mathematical statement of what said labeled feature equals in terms of the relationships between the remaining features.

4. (Original) The method in claim 2, wherein said normal system operations comprise said features in said history file at the time said models are created.

5. (Currently Amended) The method in claim 1, wherein said ~~determining~~ calculating comprises:

predicting a likelihood that said each feature will be normal when one or more of the other features are abnormal, using said model of each of said features;

repeating said predicting using different presumptions about other features being normal and abnormal to produce said trained file of a plurality of anomaly scores for each of said

features.

6. (Original) The method in claim 5, wherein said trained file provides an anomaly score for each of said features for each of a plurality of different possible abnormalities.

7. (Currently Amended) The method in claim 5, wherein said automatically identifying ~~abnormal actions~~ comprises:

determining values of said features for a given operation of said system;

referring to said trained file to retrieve an anomaly score for each of said features of said given operation;

comparing said anomaly score for each of said features of said given operation with said threshold to determine whether each anomaly score exceeds said threshold.

8. (Currently Amended) A method of automatically identifying anomalous situations during system operations, said method comprising:

recording features of normal system operations ~~actions performed by a system as features~~ in a history file;

automatically creating a model for each of said features ~~only from normal data of said normal system operations~~ in said history file;

~~determining by~~ calculating anomaly scores of said features of said normal system operations and storing said anomaly scores in to produce a trained file;

establishing a threshold to evaluate whether events in live system operations are

10/658,623

4

anomalies as compared to said normal system operations features are abnormal;

automatically identifying ~~abnormal actions~~ anomalous events in of said live system operations based on said anomaly scores and on said threshold;

reporting said anomalous event; and

periodically repeating said calculating ~~determining~~, wherein said ~~abnormal actions~~ indicate anomalous situations during system operation;

wherein said creating of said model for each of said ~~each~~ features comprises:

establishing relationships that exist between each of said ~~each~~ features for said normal system operations;

selecting a labeled feature from said features;

mathematically rearranging said relationships from the point of view of said labeled feature to create a solution for said labeled feature, wherein said solution comprises a model for said labeled feature;

selecting different features as said labeled feature and repeating said process of mathematically rearranging said relationships to produce solutions from the point of view of each remaining feature as models for the remaining features.

9. (Original) The method in claim 8, wherein said solution comprises a mathematical statement of what said labeled feature equals in terms of the relationships between the remaining features.

10. (Original) The method in claim 8, wherein said normal system operations comprise said

10/658,623

features in said history file at the time said models are created.

11. (Currently Amended) The method in claim 8, wherein said ~~determining~~ calculating comprises:

predicting a likelihood that each feature will be normal when one or more of the other features are abnormal, using said model of each of said features;

repeating said predicting using different presumptions about other features being normal and abnormal to produce said trained file of a plurality of anomaly scores for each of said features.

12. (Original) The method in claim 11, wherein said trained file provides an normally score for each of said features for each of a plurality of different possible abnormalities.

13. (Currently Amended) The method in claim 11, wherein said automatically identifying ~~abnormal actions~~ comprises:

determining values of ~~said~~ features for a given operation of said system;

referring to said trained file to retrieve and anomaly score for each of said features of said given operation;

comparing said anomaly score for each of said features of said given operation with said threshold to determine whether each anomaly score exceeds said threshold.

14. (Currently Amended) A method of automatically identifying anomalous situations during system operations, said method comprising:
- ~~recording features of normal system operations~~ actions performed by a system as features in a history file;
 - ~~automatically creating a model for each of said features of said normal system operations only from normal data in said history file;~~
 - ~~by calculating anomaly scores of said features of said normal system operations and storing said anomaly scores in to produce a trained file;~~
 - ~~establishing a threshold to evaluate whether events in live system operations are anomalies as compared to said normal system operations features are abnormal;~~
 - ~~automatically identifying abnormal actions anomalous events in of said live system operations based on said anomaly scores and on said threshold;~~
 - ~~reporting said anomalous events; and~~
 - ~~periodically repeating said calculating determining, wherein said abnormal actions indicate anomalous situations during system operations;~~
 - ~~wherein said training calculating comprises:~~
 - ~~predicting a likelihood that each feature will be normal when one or more of the other features are abnormal, using said model of each of said features;~~
 - ~~repeating said predicting using different presumptions about other features being normal and abnormal to produce said trained file of a plurality of anomaly scores for each of said features.~~

15. (Currently Amended) The method in claim 14, wherein said creating ~~said model for each said feature~~ comprises:
- establishing relationships that exist between each of said ~~each~~ features for said normal system operations;
 - selecting a labeled feature from said features;
 - mathematically rearranging said relationships from the point of view of said labeled feature to create a solution for said labeled feature, wherein said solution comprises a model for said labeled feature;
 - selecting different features as said labeled feature and repeating said process of mathematically rearranging said relationships to produce solutions from the point of view of each remaining feature as models for the remaining features.
16. (Original) The method in claim 15, wherein said solution comprises a mathematical statement of what said labeled feature equals in terms of the relationships between the remaining features.
17. (Original) The method in claim 15, wherein said normal system operations comprise said features in said history file at the time said models are created.
18. (Original) The method in claim 14, wherein said trained file provides a normally score for each of said features for each of a plurality of different possible abnormalities.

19. (Currently Amended) The method in claim 14, wherein said automatically identifying ~~abnormal actions~~ comprises:

determining values of said features for a given operation of said system;

referring to said trained file to retrieve an anomaly score for each of said features of said given operation;

comparing said anomaly score for each of said features of said given operation with said threshold to determine whether each anomaly score exceeds said threshold.

20. (Currently Amended) A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform a method of automatically identifying anomalous situations during system operations, said method comprising:

recording features of normal system operations ~~actions performed by a system as features~~ in a history file;

automatically creating a model for each of said features of said normal system operations ~~only from normal data~~ in said history file;

~~performing training by~~ calculating anomaly scores of said ~~each~~ features of said normal system operations and storing said anomaly scores in a file;

establishing a threshold to evaluate whether events in live system operations are anomalies as compared to said normal system operations ~~features are abnormal~~;

automatically identifying ~~abnormal actions~~ anomalous events in ~~of~~ said live system operations based on said anomaly scores and on said threshold;

10/658,623

reporting said anomalous events; and

periodically repeating said calculating determining, wherein said abnormal actions indicate anomalous situations during system operations.

21. (Currently Amended) The program storage device in claim 20, wherein ~~said method further comprises a process of creating a model for said each feature~~ comprises:

establishing relationships that exist between each of said each features for said normal system operations;

selecting a labeled feature from said features;

mathematically rearranging said relationships from the point of view of said labeled feature to create a solution for said labeled feature, wherein said solution comprises a model for said labeled feature;

selecting different features as said labeled feature and repeating said process of mathematically rearranging said relationships to produce solutions from the point of view of each remaining feature as models for the remaining features.

22. (Original) The program storage device in claim 21, wherein said method further comprises a mathematical statement of what said labeled feature equals in terms of the relationships between the remaining features.

23. (Original) The program storage device in claim 21, wherein said normal system

operations comprise said features in said history file at the time said models are created.

24. (Currently Amended) The program storage device in claim 20, wherein said calculating ~~rearranging~~ further comprises:

predicting a likelihood that each feature will be normal when one or more of the other features are abnormal, using said model of each of said features;

repeating said predicting using different presumptions about other features being normal and abnormal to produce said trained file of a plurality of anomaly scores for each of said features.

25. (Original) The program storage device in claim 24, wherein said trained file provides an anomaly score for each of said features for each of a plurality of different possible abnormalities.

26. (Currently Amended) The program storage device in claim 24, wherein said automatically identifying ~~abnormal actions~~ further comprises:

determining values of said features for a given operation of said system;

referring to said trained file to retrieve an anomaly score for each of said features of said given operation;

comparing said anomaly score for each of said features of said given operation with said threshold to determine whether each anomaly score exceeds said threshold.